VOLUME 17, ISSUE 1

KCJIS NEWS

JUNE 2015

INSIDE THIS ISSUE:

NEW MOBILE IDENTIFICATION TECHNOLOGY

ELY MEZA, KBI AFIS ADMINISTRATOR

The Kansas Bureau of Investigation (KBI) finalized the pilot project involving the MorphoIdent units provided by MorphoTrak.

The MorphoIdent units capture the two index-fingerprints for submission to the KBI, AFIS, and the Federal Bureau of Investigation (FBI) Repository for Individuals of Special Concern (RISC). The FBI RISC databases (housing about 2.3 million records) include: wanted persons (including the Immigration Violator File), National Sexual Offender Registry Subjects, Known or appropriately Suspected Terrorists, and other Persons of Special Interest.

The MorphoIdent units work differently from the RapID units, because they don't require an internet communication provider. Instead, they need to be interfaced to a computer (i.e. a laptop), via USB or Bluetooth connection, to forward the fingerprint captured by the MorphoIdent units to the KBI AFIS and the FBI RISC. The computer must have secured access to the KCJIS network as well as the MorphoMobile software, which will be provided by the KBI.

Once the KBI AFIS receives and processes the two-fingerprint record, it forwards the record to search the FBI RISC. Responses from the KBI AFIS and the FBI RISC are sent back to the submitting computer. The computer will be able to display the KBI and FBI responses that include personal identifiers of the individual being searched. Once the MorphoIdent unit is connected to the computer, the computer will be able to forward color coded indicators (Hit or No Hit) associated with the response messages, and the MorphoIdent user will be able to see those codes. The possible color code indicators are: ***Green light*** = No candidate; ***Yellow light*** = Possible candidate; ***Red light*** = Highly-probable candidate.

Agencies are encouraged to contact Ely Meza at (785) 296-8254 or ely.meza@kbi.state.ks.us, for any questions regarding the use of mobile identification technology. Before purchasing a mobile identification unit, KBI suggests having the vendor work with the KBI to ensure the technology meets KBI requirements.

MICROSOFT, STATE OF KANSAS, KHP REACH AGREEMENTS ON OFFICE 365

ELY MEZA, KBI AFIS ADMINISTRATOR

This past December, Microsoft Corporation, the Kansas Office of Information Technology Services (OITS), and the Kansas Highway Patrol signed agreements to begin work on a statewide implementation of Microsoft's Office 365 Government Community Cloud (GCC) and other covered services for executive branch elements of Kansas state government.

MICROSOFT, KANSAS, KHP AGREEMENT ON OFFICE 365-CONTINUED

ELY MEZA, KBI AFIS ADMINISTRATOR

Microsoft and the KHP (acting as the CJIS Systems Agency (CSA) for Kansas) agreed to a *Criminal Justice Information Services Information Agreement for Covered Services* that includes by reference and attachment the FBI CJIS Security Addendum.

It sets out agreed to controls and processes addressing many of the administrative aspects of the CJIS security policy. Because the KHP has agreed to act as the Agency Coordinator as described in FBI CJIS Security Policy 3.2.7 on behalf of all Criminal Justice Agencies in Kansas, local CJAs will be able to utilize Microsoft's Office 365 cloud services if they so choose.

This agreement between Microsoft and the KHP stipulates that each local agency will be responsible for CJIS compliance regarding how they use the Microsoft cloud services. Local agencies wishing to utilize Microsoft's cloud services will need to execute their own agreement with Microsoft in the form of a *Covered Enrolled Affiliate* Amendment to an enterprise agreement.

The logistics for completing all the tasks *including the fingerprint record checks of Microsoft personnel* have not been determined yet. CJIS security policy requires this task to be completed PRIOR to granting access to CJI.

If your agency is part of a city or county that is considering or has contracted with Microsoft for Office 365 cloud services, please contact Don Cathey dcathey@khp.ks.gov at the Kansas Highway Patrol CJIS Unit for further information and to be placed on a notification list for status updates.

DISPOSING (RETURNING) OF A FIREARM

MESSAGE KEY (QNP) TO BE MADE AVAILABLE

CARLA BOESKER, KHP CJIS SUPERVISOR

Currently law enforcement and criminal justice personnel query NCIC and/or III prior to disposing of (returning) firearms in their possession. NICS (National Instant Criminal Background Check System) is now making it possible to access NICS Index, which is a database that maintains information about persons that are prohibited the receipt/possession of a firearm in accordance with the Brady Act and NICS Regulations (e.g., illegal/unlawful aliens, mental defectives, controlled substance abusers, etc). Information in NICS Index is not available through NCIC or III.

Enabling this message key (QNP) in Open Fox will allow law enforcement/criminal justice agencies to become more effective in determining an individual's eligibility to receive/possess firearms pursuant to federal and state law. By querying the QNP message key, a search through NCIC, III and the NICS Index simultaneously will be performed. Law enforcement/Criminal Justice Agencies are not federally mandated to conduct a Disposition of Firearms (DOF) background check through NICS, however, it will be recommended.

The Kansas Highway Patrol CJIS Unit will be providing training on the proper use of the message key throughout the state, to include the Spring and Fall APCO conferences and the KCJIS Conference in June in Topeka. Once an agency has had a person(s) trained in the proper use of the message key, your agency will be allowed access to the message key. The message key will be made available to all users, regardless of training on a date yet to be determined later in the year. It is highly recommended to send personnel to training, as this message key will be subject to audit by the FBI's NICS division and KHP CJIS Unit.

KANSAS DNA DATABANK

JOHN GAUNTT, KBI BIOLOGY SECTION

Another year approached, stood by us for 52 weeks, and then passed us all by. While 2014 was with us, let's take a look at what occurred within the DNA Databank. We actually processed fewer samples in 2014: from 12,115 samples in 2013 to 11,462 samples in 2014, a decrease of about five percent (5%). We can speculate about the reasons for this decrease from a variety of angles; however, we should all know by now that the DNA Databank's mission remains as a vital lead that both the investigating agency and the victim are hoping and waiting on an unknown suspect case. When the Databank links an offender's DNA to a criminal case, we refer to it as a CODIS (Combined DNA Index System) hit.

A CODIS hit means that a DNA profile from a piece of crime scene evidence matched the DNA collected from an offender, normally collected at a booking center after a qualifying arrest. In 2014, when all of the DNA samples were processed and the required paperwork was completed, 309 criminal cases had a new investigative lead. Ten (10) homicides, 34 auto thefts, 61 sexual assaults, 29 robberies, and 140 burglaries account for 274 of the hits. These unsolved crimes are from Kansas and fifteen (15) other states. The CODIS hits increased from 300 hits in 2013.

DNA Databank received DNA samples from approximately 200 agencies during 2014. If it were not for the dedication and hard work by our booking centers, the detention staff, court service officers, community corrections staff, juvenile detention officers, correctional officers, and the offender registration staff across Kansas, those 309 criminal cases might remain unsolved.

Here is the continued challenge for our criminal justice agency partners:

Law enforcement officers take extra time to look for and collect critical biological evidence that might solve a crime.

- Any and every qualifying offender would be collected for the DNA Databank, with no exception, to the zip code or age of the offender. Kansas statute 21-2511 was revised in 2014 to clearly explain who shall be subject to DNA collection: *any adult arrested or charged or juvenile placed in custody or charged.*
- Police departments and booking centers have a plan in place to collect fingerprints and DNA from juveniles. Communication between criminal justice agencies, including the courts, seems to be the key to collect DNA on juvenile cases.

Offenders do not care about county or state lines. At some point in each offender's career, they made a calculated decision to harm another person or take another's personal property, regardless of the law enforcement agency responsible to investigate it.
Every law enforcement officer is counting on booking centers to collect DNA from qualifying offenders, because every law enforcement officer will someday investigate a crime for which he is stumped and has no further leads. [Hopefully while he was filling out the required reports, he also looked for biological evidence at the crime scene.]

Not many years ago, a responding law enforcement officer to a property crime knew that the victim needed a law enforcement case number for the insurance report. In many cases, there was not much more an officer could do for the victim. Those days have changed. During 2014, we had CODIS hits for 140 burglaries, 34 auto thefts, 9 thefts, and 4 criminal damage to property cases. Crime scene evidence could be as small as a droplet of blood or a cigarette butt. In other cases, something larger and more obvious was left behind, such as a bottle or an article of clothing. On each of those cases, the officer probably knew about the value of CODIS. But, he probably did not know when, or if the case would ever be linked to an offender in the database.

Let's have a learning lesson. There are eight misdemeanors that qualify for a DNA sample to be collected.

1. 21-5504(a)(1) or (a)(2) criminal sodomy
2. 21-5511 adultery
3. 21-5513 lewd and lascivious, in the presence of a person over 16
4. 21-5411 criminal restraint
5. 21-3513(b)(1), prior to its repeal, promoting prostitution (currently this crime is under 21-6420 and is "promoting the sale of sexual relations," but since 2103, any violation of the statute is a felony)
6. 21-6421 buying sexual relations
7. 21-5505(a) sexual battery
8. 21-6412 cruelty to animals : subsections (a)(2), (a)(3), (a)(4), (a)(5)

In 2010, a young Kansas man was arrested and charged with sexual assault. About a year later, he pled guilty to sexual battery, and

KANSAS DNA DATABANK—CONTINUED

JOHN GAUNTT, KBI BIOLOGY SECTION-CONTINUED

was placed on probation. Following this conviction, court services collected his DNA sample. Over the next couple years, his probation status was revoked a couple times. He is currently supervised by community corrections. During 2014, this same offender was linked to unsolved sexual assault in Texas. Texas law enforcement officers will no doubt make contact with him and will collect a DNA swab to be compared to the case evidence in a Texas crime lab.

What should we learn from this example?

- The booking station should have collected the DNA at the time of arrest.
- Many offenders, if given the opportunity, will plea to a misdemeanor when facing felony charges. Thankfully, this offender pled to a crime that qualified for a DNA sample.
- The court service officer did the right thing and collected the DNA sample.

When a booking agency books an offender and collects DNA, for a felony or for a qualifying misdemeanor crime, they did all that they could do. Be patient everyone. CODIS never sleeps. It just waits.

SUBMITTING ZERO REPORTS TO THE IBR UNIT

DONNA BEVITT, KBI

The monthly Zero Report is required to be submitted for every month for all agencies that do not have at least one of the following types of crimes occur:

- No IBR reportable offenses occurred
- No IBR reportable arrests occurred
- No law enforcement officers were killed or assaulted
- No homicides occurred
- No hate/bias motivated crimes occurred

A check mark or “X” should be provided in the field to the right of the type of crime if, and only if, no instance of this type of crime occurred for the month. The following example indicates that the agency had no instances of hate bias motivated crimes or homicides occurred:

Kansas Standard Offense Report (KSOR)	
Kansas Standard Arrest Report (KSAR)	
Law Enforcement Officer Killed or Assaulted (LEOKA)	
Supplemental Homicide Form	X
Hate Bias Crime	X

The Zero Report allows not only the Kansas Bureau of Investigation (KBI) but also the Federal Bureau of Investigation (FBI) to compute valid crime rates and trends and to identify months during which no criminal activity occurred. The Zero Reports also helps to identify if no crime information is being submitted by agencies and/or if none of the types of crimes did occur for the agency.

The Zero Report should be submitted by the 5th day of each month for the prior month’s data. With this in mind, let’s say you are reporting January information which is due by the 5th day of February. The date on the top of the report should be January 2015. Please do not submit a Zero Report until after the reporting month has ended. If the Zero Report is submitted prior to the end of the month it will not be entered by KIBRS staff due to the chance of incorrect submissions.

If Zero Reports are not submitted according to the requirements, it will, in turn, reflect that the agency should have all of the aforementioned types of crimes submitted for the month.

The monthly submissions of Zero Reports are required and are necessary for achieving a compliant status during the Incident Based Reporting (IBR) Section audit process. Please assist us in capturing and reporting quality data. It is our goal to provide accurate crime analysis and data to, not only the FBI, but also the citizens of Kansas.

NEWS FROM THE KBI HELP DESK

JAVIER BARAJAS, KBI HELPDESK

A KCJIS NEWSLETTER EXCLUSIVE

CJIS TOU Updates

On November 24, 2014, the KBI Help Desk and our vendor Computer Projects of Illinois (CPI) implemented updates associated with Technical and Operational Update, TOU 14-1 through TOU 14-6. TOU 14-7 and TOU 14-8 were also implemented on February 1, 2015. TOU 14-9 required no changes to the Central Message Switch. As of February 2015 Kansas is up to date on NCIC TOUs. For details on TOUs please visit the KCJIS Web Portal Information tab and click on the NCIC Manual link under the Federal Systems section. A complete list of TOU's issued by NCIC is available for your review.

Q

On a Master Search on the KCJIS Web Portal, can the name of the subject searched be included when the result is 'No Persons Match Your Criteria?'

A

The KCJIS Web Portal has been updated so when a search is submitted, the information of the search is included on the results page. The time of search, Purpose Code, User ORI, User ID, Initiated For, Last Name, First Name and Data Sources are all included on the results page.

Retired Nlets Bulk Cash Smuggling BCQ

Effective 7/9/2014, the Department of Homeland Security/Homeland Security Investigations (DHS/HSI) Bulk Cash Smuggling Center (BCSC) has discontinued its support of the BCQ Bulk Cash Smuggling message key. Requests will return a canned response asking you to contact the BCSC directly by phone 1-866-981-5332 or via an administrative (AM) message to ORI VTICE1600. The KBI Help Desk has removed access to the BCQ message key from the Central Message Switch. Contact your Computer Automated Dispatch (CAD) vendor to remove this message key if it is still available in their software.

KCJIS User Group

During the December meeting in Topeka the KCJIS User Group enjoyed a presentation by Matt Billinger from Kansas Department of Corrections (KDOC) on Interstate Compact. During his presentation it brought up that something should be included in the miscellaneous section on an entry so agencies are aware. Here is what Matt's office provided as a suggestion to include: “Offender is being supervised by Kansas Parole under the Interstate Compact of Adult Offender Supervision of supervision. The supervising officer has valid waiver of extradition for any out of state warrant. While a preliminary hearing may be held before retaking, a fugitive from justice warrant may not be necessary.” Please contact the local Parole Office or kscompact@doc.ks.gov for more information. (www.interstatecompact.org)”

KCS – Kansas Tag

When running a Kansas tag via Kansas Car Stop (KCS), the license type (LIT) field must be blank and the special issue tag (SIT) field can be left blank or the SD code may be submitted.

Messenger 3.0 Upgrade

The upgrade to OpenFox Desktop and OpenFox Messenger version 3.0 introduces many new and useful features. The KBI Help Desk and Computer Projects of Illinois, CPI implemented this upgrade on February 1, 2015. Below is a list of highlights that you may notice with the upgrade.

Messenger 3.0 Upgrade

The upgrade to OpenFox Desktop and OpenFox Messenger version 3.0 introduces many new and useful features. The KBI Help Desk and Computer Projects of Illinois, CPI implemented this upgrade on February 1, 2015. Below is a list of highlights that you may notice with the upgrade.

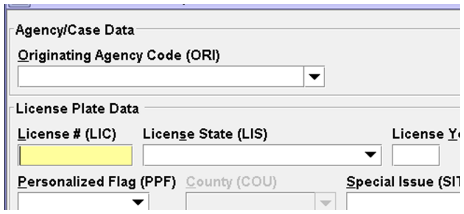
NEWS FROM THE KBI HELP DESK—CONTINUED

JAVIER BARAJAS, KBI HELPDESK

Messenger 3.0 Upgrade

The upgrade to OpenFox Desktop and OpenFox Messenger version 3.0 introduces many new and useful features. The KBI Help Desk and Computer Projects of Illinois, CPI implemented this upgrade on February 1, 2015. Below is a list of highlights that you may notice with the upgrade.

- Desktop Enhancements
  - *Enhanced Focus Indicator* – This feature makes it much easier for you to immediately tell what field is the currently focused field. By default, Desktop highlights the focused field in a yellow color.



Agency/Case Data

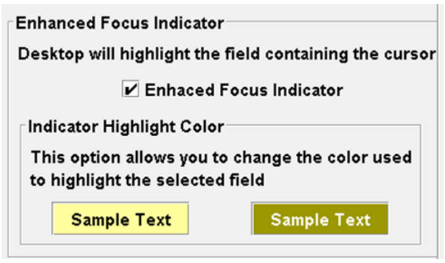
Originating Agency Code (ORI)

License Plate Data

License # (LIC) License State (LIS) License Y

Personalized Flag (PPF) County (COU) Special Issue (SI

You can modify this color in your preferences screen. Within Messenger, click Tools, User Preferences. The Modify User Preferences screen will default to Desktop General. However, you can navigate back to this screen by clicking the Desktop icon from the top menu pane and General icon within the left menu pane. The 'Enhanced Focus Indicator" section allows you to change the color used to highlight the selected field.



Enhanced Focus Indicator

Desktop will highlight the field containing the cursor

☑ Enhaced Focus Indicator

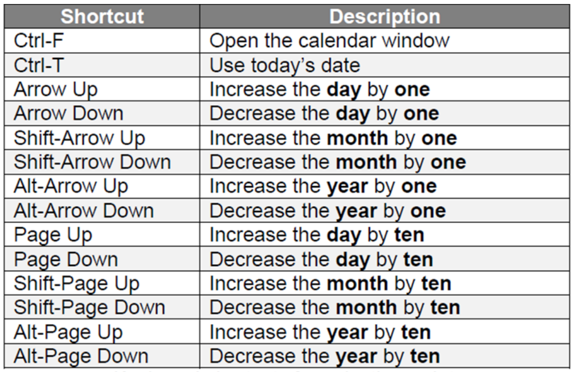
Indicator Highlight Color

This option allows you to change the color used to highlight the selected field

Sample Text Sample Text

- *Diagnostic Request Message* – The KBI Help Desk now has the ability to generate a Desktop Diagnostic Message. This feature is intended for use in providing support. Help Desk Technicians can automatically request the diagnostic information, instead of walking you through steps to gain the same information. Information gathered from a Diagnostic Message can include User and Station Ids, versions of many elements associated with OpenFox Desktop such as Java and Messenger as well as other modules for a particular station ID.

- *Date Field Enhancements* – You now have access to several additional keyboard shortcuts that make the process of entering date fields much easier. From within a date field, you can hold Ctrl and hit T to populate the field with the current date. See the table below to change the date value of the date field.



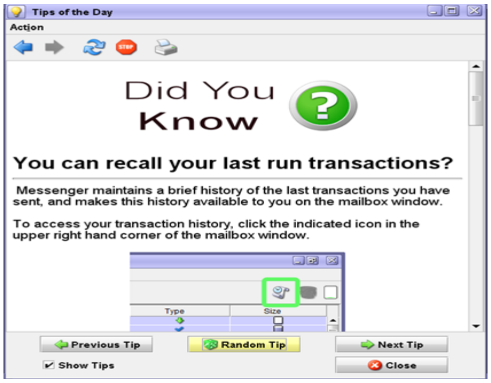
Shortcut	Description
Ctrl-F	Open the calendar window
Ctrl-T	Use today's date
Arrow Up	Increase the **day** by **one**
Arrow Down	Decrease the **day** by **one**
Shift-Arrow Up	Increase the **month** by **one**
Shift-Arrow Down	Decrease the **month** by **one**
Alt-Arrow Up	Increase the **year** by **one**
Alt-Arrow Down	Decrease the **year** by **one**
Page Up	Increase the **day** by **ten**
Page Down	Decrease the **day** by **ten**
Shift-Page Up	Increase the **month** by **ten**
Shift-Page Down	Decrease the **month** by **ten**
Alt-Page Up	Increase the **year** by **ten**
Alt-Page Down	Decrease the **year** by **ten**

Keyboard shortcuts for selecting a date

NEWS FROM THE KBI HELP DESK—CONTINUED

JAVIER BARAJAS, KBI HELPDESK

- Messenger Enhancements
    - *Tip of the Day* – The tip of the day will automatically open in a window within OpenFox Messenger with a handy tip. You can view more tips by clicking the Previous Tip, Next Tip or Random Tip buttons. If you do not want the Tip of the Day window to show you can unselect the 'Show Tips' checkbox before clicking the Close button.

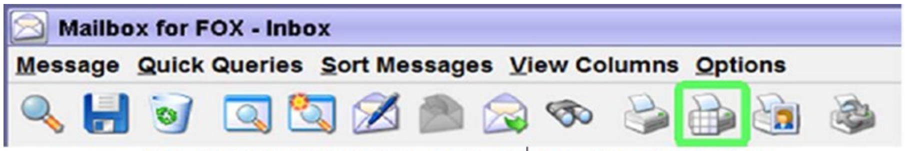


You can recall your last run transactions?

Messenger maintains a brief history of the last transactions you have sent, and makes this history available to you on the mailbox window.

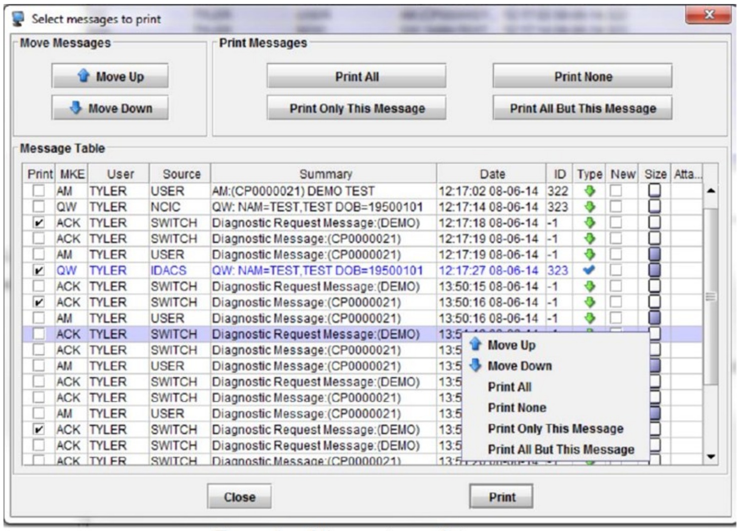
To access your transaction history, click the indicated icon in the upper right hand corner of the mailbox window.

- *Custom Print* – The custom print feature provides greater control over the format of your print outs from Messenger. You can choose what messages are printed and the order in which they are printed. For example, a dispatcher may use this feature when they run a query that results in five different returns; however, the dispatcher only wants to print the NCIC return.



The custom print button. You can also press Ctrl-Alt-P

Clicking on the highlighted button above opens the custom print window. A window will open and list the messages you highlighted in your inbox. You can then select which messages to print by checking or unchecking the box under the Print column. You can also change the order the of print outs with the Move Up and Move Down buttons.



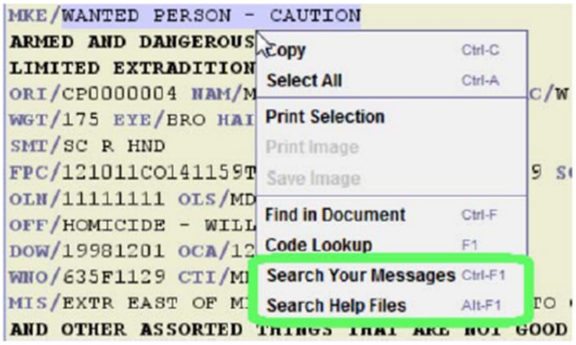
Print	MKE	User	Source	Summary	Date	ID	Type	New	Size	Atta...
□	AM	TYLER	USER	AM:(CP0000021) DEMO TEST	12:17:02 08-06-14	322	⬇	□	□	
□	QW	TYLER	NCIC	QW: NAM=TEST,TEST DOB=19500101	12:17:14 08-06-14	323	⬇	□	□	
☑	ACK	TYLER	SWITCH	Diagnostic Request Message:(DEMO)	12:17:18 08-06-14	-1	⬇	□	□	
□	ACK	TYLER	SWITCH	Diagnostic Message:(CP0000021)	12:17:19 08-06-14	-1	⬇	□	□	
□	AM	TYLER	USER	Diagnostic Message:(CP0000021)	12:17:19 08-06-14	-1	⬇	□	■	
☑	QW	TYLER	IDACS	QW: NAM=TEST,TEST DOB=19500101	12:17:27 08-06-14	323	✓	□	■	
□	ACK	TYLER	SWITCH	Diagnostic Request Message:(DEMO)	13:50:15 08-06-14	-1	⬇	□	□	
☑	ACK	TYLER	SWITCH	Diagnostic Message:(CP0000021)	13:50:16 08-06-14	-1	⬇	□	□	
□	AM	TYLER	USER	Diagnostic Message:(CP0000021)	13:50:16 08-06-14	-1	⬇	□	■	
□	ACK	TYLER	SWITCH	Diagnostic Request Message:(DEMO)	13:5				□	
□	ACK	TYLER	SWITCH	Diagnostic Message:(CP0000021)	13:5				□	
□	AM	TYLER	USER	Diagnostic Message:(CP0000021)	13:5				■	
□	ACK	TYLER	SWITCH	Diagnostic Request Message:(DEMO)	13:5				□	
□	ACK	TYLER	SWITCH	Diagnostic Message:(CP0000021)	13:5				□	
□	AM	TYLER	USER	Diagnostic Message:(CP0000021)	13:5				■	
☑	ACK	TYLER	SWITCH	Diagnostic Request Message:(DEMO)	13:5				□	
□	ACK	TYLER	SWITCH	Diagnostic Request Message:(DEMO)	13:5				□	
□	ACK	TYLER	SWITCH	Diagnostic Message:(CP0000021)	13:5				□	

Example of the custom print screen

NEWS FROM THE KBI HELP DESK—CONTINUED

JAVIER BARAJAS, KBI HELPDESK

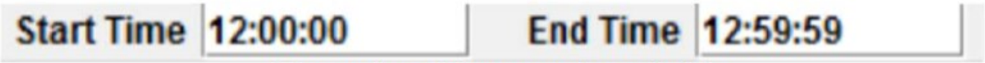
- *Preview Pane Enhancements* – You can now highlight text in the Messenger preview pane and then search for that text in your Messenger messages or in the help files. To do this, simply highlight the text in the preview pane and then right click. Choose the appropriate item from the popup menu.



```
MKE/WANTED PERSON - CAUTION
ARMED AND DANGEROUS
LIMITED EXTRADITION
ORI/CP0000004 NAM/M                          C/W
WGT/175 EYE/BRO HAI
SMT/SC R HND
FPC/121011CO141159T                          9 S
OLN/11111111 OLS/MD
OFF/HOMICIDE - WILL
DOW/19981201 OCA/12
WNO/635F1129 CTI/MI
MIS/EXTR EAST OF MI                          TO
AND OTHER ASSORTED THINGS THAT ARE NOT GOOD
```

- Archive and Retrieval
  - *Time Format* – The start time and end time fields now use a formatted display to make them more readily understood.

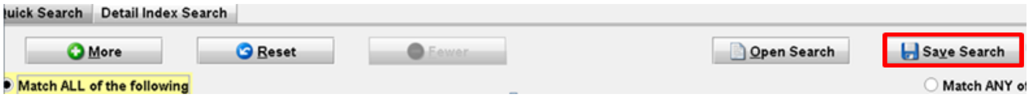
Several convenience methods have also been added to these fields. First, you can choose to only enter the hour value and then Archive & Retrieval defaults the minutes and seconds to all zeros. Before you would have needed to manually fill in the zeros. Secondly, you may use keyboard shortcuts to alter the time. See *Date Field Enhancements* above.



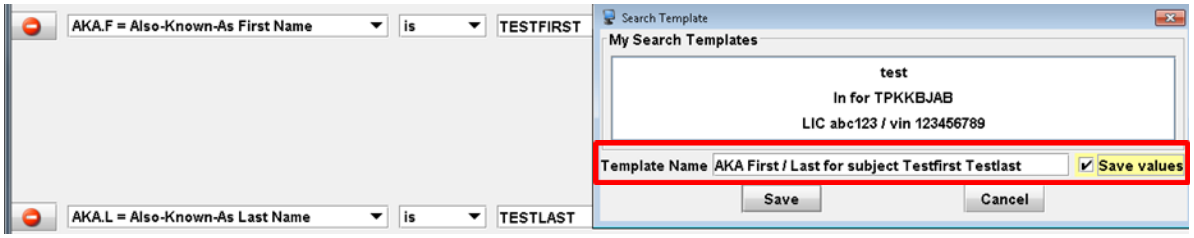
Start Time 12:00:00 End Time 12:59:59

Example of the new time fields

- *Search Templates* – Archive & Retrieval allows you to save previous searches as search templates. You can then reuse these templates in the future for your commonly run Archive searches. From the Detail Index Search tab, set your search criteria as you normally would for an Archive search. Click the Save Search button.



The Search Template window will popup. Name the template and click the Save button. If you want the values saved in the template, check the Save Values checkbox.



AKA.F = Also-Known-As First Name ▾ is ▾ TESTFIRST

AKA.L = Also-Known-As Last Name ▾ is ▾ TESTLAST

Search Template

My Search Templates

test

In for TPKKBJAB

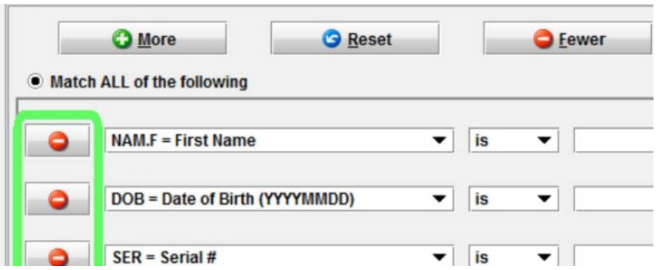
LIC abc123 / vin 123456789

Template Name AKA First / Last for subject Testfirst Testlast ☑ Save values

NEWS FROM THE KBI HELP DESK—CONTINUED

JAVIER BARAJAS, KBI HELPDESK

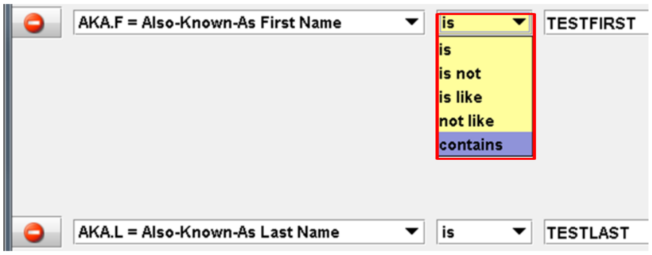
- *Details Search* – The details search screen now allows you to remove any criteria row from the search screen. Previously, you would only be able to remove the last criteria row by clicking on the Fewer button. Now, clicking on the delete button next to each row will remove that row of criteria.



● Match ALL of the following

NAM.F = First Name | is
DOB = Date of Birth (YYYYMMDD) | is
SER = Serial # | is

- *New Search Condition* – The search condition is the second drop down list on each row. This drop down allows you to choose how the search fields must match.


AKA.F = Also-Known-As First Name | is | TESTFIRST

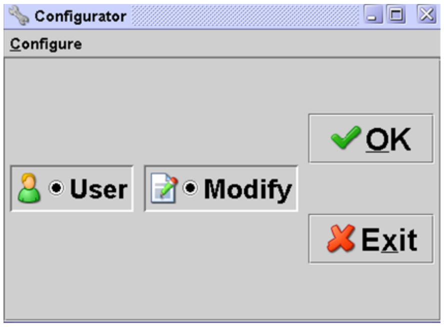
AKA.L = Also-Known-As Last Name | is | TESTLAST

The new 'contains' condition looks for text anywhere within the field: at the start, at the end, or in the middle.

- *Auto-change to 'is like' Search Condition* – Archive & Retrieval has been enhanced so that if you enter a wildcard character into the search field, the client automatically changes the search condition to 'is like'. Previously, you would have to remember to change the condition to 'is like' if you wanted to search by wildcard.

OpenFox Configurator

This final change was not part of the Messenger 3.0 upgrade, however, it does clear a few unnecessary options. The OpenFox Configurator screen has changed to only show the objects you have access to. For example, as a Terminal Agency Coordinator (TAC) you are allowed to modify users within your agency. The Configurator screen will no longer show you all objects available, but only the User and Modify objects. Hopefully, this will be a little clearer for TACs accessing Configurator.



ACCESS TO CJI AND THE PAPERWORK REQUIRED TO GET IT

DON CATHEY, KHP KCJIS INFORMATION SECURITY OFFICER

The FBI CJIS Audit Unit's Information Technology Security Audit (ITSA) conducted during August 2014 discovered there is still confusion about what paperwork is needed for the various scenarios where access is granted to Criminal Justice Information (CJI) or systems used to access CJI. Recent changes to some policy and related definitions have only added to the muddy waters. The following recommendations were among those made to the Kansas Highway Patrol.

- *Ensure the local agencies implement appropriate* ***agreements*** *with their respective noncriminal justice agencies. (This was a recommendation during the previous audit cycle.)*

This recommendation refers to Policy 5.1.1.4.

- *Ensure the local agencies implement the* ***CJIS Security Addendum*** *with their servicing private contractor personnel. (This was a recommendation during the previous audit cycle.)* This recommendation refers to Policy 5.1.1.5.

These recommendations differ based on WHO is accessing CJI and HOW those personnel are controlled by the criminal justice agency. Answering two questions may help to determine the proper agreement required.

Who gives the person getting access their annual performance review?

- The person is reviewed within your agency – no extra agreement needed.
- If the person's review is completed by a different governmental agency and your agency does not have direct input into that process. – That is an inter-agency AGREEMENT.
- Their review (if any) is done by a private sector company and your agency has no direct input in that process. – That requires the FBI CJIS Security Addendum.

How do you enforce the conditions or settle any disputes over parts of the pact?

- If all issues are settled within your agency with final determinations made by your agency head – no special agreements are needed.
- If you take up any matters with a government department head, city council, or county commission - that is an Inter-Agency agreement.
- If you file suit and go before a judge in court – that is contractual dispute with a private contractor. Your original contract for services needs to include the FBI CJIS Security addendum by reference.

The KCJIS 218 form available on the Kansas Highway Patrol CJIS Launch Pad is similar to an example provided in the FBI CJIS Security Policy Appendix D. It is intended as one way to fulfill the requirement of policy 5.1.1.4.

The FBI CJIS Security addendum required by policy 5.1.1.5 is published in Appendix H of the FBI CJIS Security Policy. It can only be changed with FBI approval. However, they have allowed minor modifications for some contractor scenarios. If your contractor is reluctant to include the security addendum as published, contact your agency's technical security auditor to discuss the issues and solutions.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Proper use and compliance with policy regarding these agreements is vital to ensuring all parties fully understand and agree to a set of security standards.

INFORMATION TECHNOLOGY SECURITY AUDIT REPORT RECEIVED

DON CATHEY, KHP KCJIS INFORMATION SECURITY OFFICER

In August 2014, the FBI's CJIS Audit Unit (CAU) conducted several audits involving Kansas Criminal Justice Agency use of FBI criminal justice information systems. One of those audits focused on compliance to the FBI CJIS Security Policy and how Kansas agencies protect Criminal Justice Information as well as the systems used to access CJI. The "ITSA" audit team visited the KHP, KBI, and fourteen local agencies. I have included excerpts from their report.

While the audit did not find any glaring problems, they did find some areas where they made recommendations for improvement, many of which had been identified in previous security audits. The Audit Recommendations will be forwarded to the APB Compliance Evaluation Subcommittee for follow-up actions. The Areas of Concern are things needing to be addressed by the next audit cycle. I have edited some of the language and format for emphasis and to fit this article.

Audit Recommendations

Based on the ITSA conducted during August 2014, the FBI's CJIS Division made the following recommendations to the Kansas Highway Patrol.

1. ***Ensure the local agencies implement appropriate agreements with their respective noncriminal justice agencies. (This was a recommendation during the previous audit cycle.)***
2. ***Ensure the local agencies implement the CJIS Security Addendum with their servicing private contractor personnel. (This was a recommendation during the previous audit cycle.)***
3. ***Ensure the CSA and the local agencies fingerprint all agency terminal operators, IT personnel, noncriminal justice agency personnel, and unescorted custodial, support, and contract personnel with access to CJI.***
4. ***Ensure the local agencies provide security awareness training to all agency terminal operators, IT, noncriminal justice agency and private contractor personnel who manage and/or have access to CJI within six months of assignment and/or at least once every two years. (This was a recommendation during the previous audit cycle.)***
5. ***Ensure the local agencies' passwords used for authentication follow the secure password attributes. (This was a recommendation during the previous audit cycle.)***
6. ***Ensure the local agencies log successful and unsuccessful logon attempts and password changes.***
7. ***Ensure the local agencies encrypt all network segments that access CJI with at least 128-bit NIST certified encryption to comply with the FIPS 140-2 requirement. (This was a recommendation during the previous two audit cycles.)***

New Policy Overview

The CJIS Security Policy contains new requirements for agencies to implement. These new policy requirements, although assessed, will not be forwarded through the APB Compliance Evaluation Subcommittee during the current zero cycle audit that is specified with "required by" and the year. The intent is for agencies to start working toward compliance immediately, where possible. The audit, as well as the Requirements and Transition Document, can be used as a tool for financial planning and justification to meet these new requirements. Adherence to all new policies and procedures is required for FBI CJIS systems access.

New Policy: Areas of Concern (Zero Cycle)

Although not recommendations at this time, the following Areas of Concern were identified:

1. ***Ensure the local agencies provide the first tier of security awareness training to all unescorted personnel with access to CJI.***
2. ***Ensure the local agencies protect and control electronic and physical media during transport.***

INFORMATION TECHNOLOGY SECURITY AUDIT REPORT—CONTINUED

DON CATHEY, KHP KCJIS INFORMATION SECURITY OFFICER

3. *Ensure the local agencies display an approved system use notification message on all information systems accessing CJI.*
4. *Ensure the CSA and local agencies validate system accounts at least annually and document the validation process.*
5. *Ensure the CSA and the local agencies implement all audit and accountability controls for information systems accessing CJI.*

The KHP CJIS Unit will continue our efforts to Inform, Explain and Clarify security policies.

You can help by:

- Studying articles about these recommendations and other security topics appearing in this and future *KCJIS newsletters*.
- Participate in Local Agency Security Officer (LASO) training. The curriculum and delivery methods are reviewed annually to ensure topics are presented as completely and clearly as possible.
- Respond to audit questionnaires, when the time comes, in a timely manner to allow everyone to review and evaluate your agency's security practices in an orderly and complete fashion.
- Should an issue be discovered during a KHP Information Security Audit, correct it as soon as possible.
- Use the latest forms available on the KHP CJIS Launch Pad when requesting approvals for new connections or changes. Forms are reviewed and modified to reflect the changing needs for information to ensure compliance with the latest security policies.
- Complete the forms as completely and accurately as possible.

Together, the KCJIS community will succeed in making our systems secure by following these recommendations along with all the other CJIS security policies.

KANSAS INCIDENT BASED REPORTING SYSTEM: DATA SUBMISSION DEADLINES FOR 2015

JANELL ZEILER, KBI IBR UNIT

The Incident Based Reporting Section at the Kansas Bureau of Investigation has released the 2015 deadline schedule for submitting Kansas Standard Offense and Arrest data to the KBI. These dates also represent the deadline for submitting the *Law Enforcement Officers Killed and Assaulted (LEOKA) report*, *Supplemental Homicide Reports* and the *Zero Report*.

- **April 10, 2015:** First Quarter deadline. Submit a January-March 2015 data to the KBI headquarters.
- **July 10, 2015:** Mid-Year deadline. Submit a January- June 2015 data to the KBI headquarters. This is the deadline to be included in semi-annual statistic reports.
- **October 9, 2015:** Third Quarter deadline. Submit a July- September 2015 data to the KBI headquarters.
- **January 15, 2016:** Fourth Quarter deadline. Submit a January- December 2015 data to the KBI headquarters. This is the deadline for your agency to be included in the FBI *Crime in the United States* publication and other annual statistic reports.

HOW SECURE IS MY PASSWORD?

TAMMIE HENDRIX, KHP TECHNICAL SECURITY AUDITOR

News reports continue to indicate one of the vulnerabilities most widely used by hackers is a weak password.

Here are a few tips to create a secure and memorable password:
Remember, the longer the password the more secure it is likely to be. Create a password that has at LEAST eight or more characters (this is the minimum for KCJIS users, but LONGER is STRONGER).

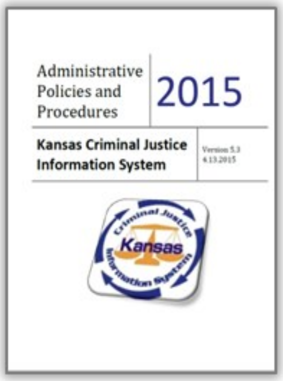
Things to avoid: Names, places, dictionary words.

- Use a different password for each of your important accounts, like your email and online banking accounts. Re-using passwords is risky. If someone figures out your password for one account, that person could potentially gain access to your email, address, and even your money.
- Change your password often. If someone has figured out your password, they might be accessing your account without you knowing. Regularly changing your password helps limit this type of unauthorized access.
- Use a mix of letters, numbers, and symbols in your password. Using numbers, symbols and mix of upper and lower case letters in your password makes it harder for someone to guess your password. For example, an eight-character password with numbers, symbols and mixed-case letters is harder to guess because it has 30,000 times as many possible combinations than an eight-character password with only lower case letters.
- Don't use personal information or common words as a password. Create a unique password that's unrelated to your personal information and uses a combination of letters, numbers, and symbols. For example, you can select a random word or phrase and insert letters and numbers into the beginning, middle, and end to make it extra difficult to guess (such as "sPo0kyh@ll0w3En"). Don't use simple words or phrases like "password" or "letmein," keyboard patterns such as "qwerty" or "qazwsx," or sequential patterns such as "abcd1234" which make your password easier to guess.
- Keep your passwords secure.
- Make sure to regularly update your recovery email address so that you can receive emails in case you need to reset your password. You can also add a phone number to receive password reset codes via text message.
- Many websites will also give you the option of answering a security question if you forget your password.
- If you have to choose a question from a list of options, such as the city where you were born, try to find a way to make your answer unique by using some of the tips above. That way even if someone guesses the answer, they won't know how to enter it correctly.
- If you can create your own question, consider these tips to come up with a question that has an answer only you would know:
    - Make it safe: The answer shouldn't be something that someone can guess by scanning information you've posted online on blogs or social networking profiles.
    - Make it Memorable: If you can't remember the answers to your security questions, you have achieved nothing.
    - Make it the Answer Consistent: The answers should not change over time. For instance, asking "What is the name of your significant other?" may have a different answer 5 years from now. But "What is the last name of your 6th grade teacher?" is historical and not going to change.

If you're curious whether your password is secure or not, run it through an online password checker like:
http://online-domain-tools.com/ or https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

NEW KCJIS POLICIES AND PROCEDURES NOW AVAILABLE

DON CATHEY, KHP KCJIS INFORMATION SECURITY OFFICER


Administrative Policies and Procedures
2015
Kansas Criminal Justice Information System
Version 5.3
4.13.2015
Criminal Justice
Kansas
Information System

On Monday, April 13, 2015, the KCJIS committee approved a revised KCJIS policies and procedures manual after a few minor corrections. Those corrections have been made and the revised policy is now available from the CJIS documents or the CJIS manuals areas of the Kansas Highway Patrol CJIS launch pad. https://cjisaudit.khp.ks.gov/launchpad

It has also been posted to the KCJIS secure web portal. Under the information menu, scroll down to the security policies.

This version of KCJIS policies and procedures covers changes in FBI CJIS Security Policy version 5.3. It maintains the 3 part format of recent versions. Part One is the FBI CJIS Security Policy. Part Two includes KCJIS specific policies and any enhancements to FBI policy. And Part Three is a guidance section.

FBI and KHP CJIS auditors deal with changes that make stronger policies in the same way. If a new policy creates a new requirement, that requirement is considered to be a “zero cycle” audit item until it has been introduced to local agencies through a full audit cycle (3 years). That means the first audit conducted after it becomes policy will be used for education and training on that specific requirement without any sanction or other actions by the auditor.

In attempts to keep policy current regarding technology trends and advancements, the FBI intends to publish annual updates to their security policy. The next FBI update (version 5.4) is likely to be released later this summer. The KCJIS policy subcommittee will be back to work soon, beginning to compare our newest version to upcoming changes from the FBI.

Input from the KCJIS user community is welcome. In fact, we have developed a policy review process to be used to make recommendations and requests for policy changes.

Instructions along with a standardized form are located on the KHP CJIS Launch Pad at: https://cjisaudit.khp.ks.gov/launchpad/cjisdocs/files/kcjis_policy_review_request_distributed.pdf

When policy changes, the KHP CJIS unit also reviews our KCJIS forms to make sure they are keeping with the latest requirements.

For example, the KCJIS 208 has been revised to reflect that it is no longer required to be signed every other year as part of the 1st level of security awareness training and therefore is no longer an instructional tool with security awareness topics.

Other forms are changed to ensure new information is gathered as needed to determine compliance status as FBI or KCJIS policies change. Some are updated for ease of completion.

So always be sure to use the latest forms when requesting new KCJIS devices or other changes. Forms can be found on the KHP CJIS Launch Pad inside the CJIS Forms folder with the CJIS documents area.

CLICK IT AND TROUBLE TICKET

KIP BALLINGER, IT SECURITY AUDITOR / TRAINER; KHP CJIS UNIT

If you click on it, you may be opening a trouble ticket! In my role as a KCJIS Security Auditor, as technology is ever-advancing, I seek to keep up-to-date with emerging technologies and current developments in the I.T. world. I spend a portion of my time reviewing published security reports that provide statistical data and identify information system security concerns, such as shifts in malware, trends in vulnerabilities, as well as best practices for avoiding these threats. I would like to share some of these highlights with you.

Palo Alto Networks, in the their publication, *ThreatTrend – Threat Landscape Review*, has found that 87% of malware arrives via SMTP (email) 11.8% via HTTP (web), and only 1.2% via the remaining applications. In other words, nearly 99% of malware is delivered through email and Web-Browsing. SMTP is the protocol used to transmit e-mails from one location to another, and Web-Browsing - a broad category to describe web (HTTP) traffic, e.g. Facebook or Gmail. The report also noted that the majority of the malware detected in the sample data was delivered in the form of a Windows executable (either an EXE or DLL file), with a much smaller percentage (0.8%) delivered as a Microsoft Office document and the remaining file types making up just 0.1%.

In their report, *2015 Internet Security Threat Report: The Cyber Landscape*, Symantec, based on prohibited websites blocked by users of Symantec products, identified potential risk sources that may arise from uncontrolled use of Internet resources. The data from 2014 indicated that the most frequently blocked traffic was categorized as social networking, followed by advertisements and pop-ups. Web-based advertisements pose a potential risk through the use of 'malvertisements', or malicious advertisements. These may occur as the result of a legitimate online ad provider's being compromised or a banner ad being used to serve malware on an otherwise harmless website.

Malware developers know what they are doing and they present their product right where potential victims are most likely to click on it – email and web browsers. ***And if you click it, you'll be opening a trouble ticket!*** Hackers and scam artists try to trick people into clicking on links that will download malware and spyware to their computers, especially computers that don't use adequate security software. Yet even with security software, the best bet is to avoid malware by not clicking on anything unless you were expecting it in advance and know the person sending it. This practice will greatly reduce your risk of downloading unwanted malware and spyware.

...the vast majority (of malware) are installed by some action from a user, such as clicking an e-mail attachment or something on a web page

Malware is a term for malicious software – a broad class of software, which includes viruses, worms, Trojans, and bots, back doors, spyware, and adware. This software or malicious code is specifically designed to harm, interrupt, steal, or in general cause some other harmful or illicit action to the software, data, computers, or networks. There are many ways malware can infect your computer.

Some are bundled with other programs or attached as macros to files. Some arrive by exploiting a known vulnerability in an operating system, network device, or other software. *However, the vast majority are installed by some action from a user, such as clicking an e-mail attachment or something on a web page,* or by downloading a file from the Internet. And if you click it, you'll be opening a trouble ticket!

Here are a few tips in avoiding malware:

- Keep your software updated, i.e., be aggressive in your updating and patching. This includes software on the computers and IOS firmware on network devices. Your computer(s) should have anti-virus and anti-spyware (malware) software, as well as a firewall. Set your operating system and security software to update automatically.

- Instead of clicking on a link in an email, type the URL you know is legitimate for the site you want directly into your browser. The links may look legitimate and appear to be from someone you know and trust, but clicking on them could download malware or send you to a spoof site designed to steal your personal information.

CLICK IT AND TROUBLE TICKET– CONTINUED

KIP BALLINGER, IT SECURITY AUDITOR / TRAINER. KHP CJIS UNIT

Download and install software only from websites you know and trust. Free programs can be enticing, but free software often includes bundled applications of multiple programs and can come with malware. *Never download software in response to unexpected pop-up messages or emails, especially ads that claim to have scanned your computer and detected malware.*

> *Free programs can be enticing, but free software often includes bundled applications of multiple programs and can come with malware.*

Website ‘popup’ alerts deceive the user by claiming that their machine is infected with a virus or has some other problem that needs to be fixed. By clicking on the alert, the user will either be asked to install the software that is purported to fix the issue, which is really malware in disguise, or else a ‘drive-by’ download will be initiated – that is - a script on the site secretly runs and installs malware when you visit a website. Many other website ads are designed to persuade the user to click on the ad or on a ‘close’ button. When the user obliges, a ‘drive-by’ download is initiated. Make sure your browser security setting is high enough to detect unauthorized downloads.

Other measures you can take to avoiding malware include deploying a web browser URL reputation plug-in solution that displays the reputation of websites highlighted during web searches. Another is to scan all downloaded files for malware before opening.

Your anti-malware/anti-virus software should perform full system scans at least weekly. Does your anti-virus software scan the computers “root”? Not all do. The “root” lies outside of the operating system and is a prime location for attackers to hide their malware. There are a number of programs that can provide root scans and monitor the root area. And finally, have a backup-and-restore plan in place in the event of a successful attack or catastrophic data loss.

Think twice before you ‘click it’. If you click on it and you’re wrong, you are in for trouble!

NEW WARNINGS RELEASED THAT MAY AFFECT YOU AND YOUR FAMILIES

DON CATHEY, KHP KCJIS INFORMATION SECURITY OFFICER

As part of my attempts to comply with CJIS security policy **5.10.4.4 Security Alerts and Advisories**, I subscribe to the US-Computer Emergency Readiness Team (US-CERT) email notifications. As such, I recently received the following alert. The information contained in the links is good practice for everyone to follow.

> National Cyber Awareness System:
>
> IC3 Warns of Cyber Attacks Focused on Law Enforcement and Public Officials
>
> *04/21/2015 09:33 PM EDT*
> Original release date: April 21, 2015
> The Internet Crime Complaint Center (IC3) has issued an alert warning that law enforcement personnel and public officials may be at an increased risk of cyber attacks. Doxing—the act of gathering and publishing individuals’ personal information without permission—has been observed. Hacking collectives may exploit publicly available information identifying officers or officials, their employers, and their families. These target groups should protect their online presence and exposure.
> Users are encouraged to review the IC3 Alert for details and refer to US-CERT Tip ST06-003 for information on staying safe on social network sites.

In case you are reading this article "offline", here are the respective Universal Resource Locators (URL) s for the links in the last portion of the alert. You can enter them on the address line of your computer’s internet browser (without the **bold** I’ve added for identification) for more information and tips:
http://www.**ic3**.gov/media/2015/150421.aspx and https://www.**us-cert**.gov/ncas/**tips/ST06-003**

For more information about US-CERT go to https://www.us-cert.gov/about-us.

KBI BIOLOGY/DNA DATABANK

JOHN GAUNTT, KBI BIOLOGY SECTION

Once in a while, I will hear about a phone call, an email message, or a conversation about a local agency's remark, "I didn't think the KBI lab worked property crimes." Usually I stop and wonder if I heard that remark correctly. I recognize that there obviously is some doubt among our contributors, and the right thing to do is to communicate more effectively about property crimes.

This newsletter is a great opportunity to dispel some misunderstandings. In short, KBI laboratories welcome property crime evidence submissions. They always have, and always will, as embodied in the KBI mission statement to provide laboratory service to criminal justice agencies. So how did the confusion get started?

Several years ago, the laboratory announced certain evidence guidelines for biology type cases; and again this past year with the rollout of the biology submission form that is required to accompany evidence upon submission to the Evidence Control Center. Biologists have determined that some types of items and exams are not going to give satisfactory results to the submitting agency. Here are the identified types of items that cannot be processed for biology:

- drug baggies /packaging
- live ammunition
- fired handgun and rifle shell casings

Most of these are readily understood. What is another available option for a submitter with drug packaging evidence? Why not consider a latent print exam for the packaging? Loaded and fired ammunition can also be checked for latent prints. Did you deduce that fired shotgun rounds could be processed for biology? Good job. Yes, biologists will accept fired shotgun shells.

Now, for the loud thud. In 2011, the KBI wrote to agencies that *touch DNA* evidence would not be accepted on property crimes, stating that "touch DNA samples seldom yield sufficient DNA profiles for associating an individual to a crime". Before you sigh and stop reading any further, please continue just for a little bit.

Touch DNA is one of several descriptive terms for short time contact with a surface. Not being an examiner, I definitely would not make conclusions about workable DNA profiles from a suspect's short time contact with a surface. But from what I understand in almost eight years in the Biology Section, swabs of touch DNA are not worth the time and expense to work. On an average case, the laboratory was receiving this type of evidence:

- from a car burglary – swabs from the console latch or glove compartment
- home burglary – swabs of doorknobs, light switches, drawer handles, connections on electronics
- auto thefts – swabs from the car's gearshift and steering wheel
- business burglary – swabs from outer door, interior doorknobs, desk drawers, cash register keys

If you think about each case individually, whose DNA profile would most likely be swabbed on any these examples? Answers: the regular car driver; the home owner / residents; the regular car driver; and the employees of the business.

What were the results of the 2011 letter? The announcement decreased the number of property crime submissions for biology testing. Latent prints also received fewer submissions. A coincidence? Probably not.

We are asking agencies to look for quality biology type evidence on these property crimes that can **identify** the offender through DNA. Here are some worthwhile submissions that will put both a smile on the examiner's face and also on the submitting agency's face when the lab results are sent:

- the filter / butt from a smoked cigarette

KBI BIOLOGY/DNA DATABANK – CONTINUED

JOHN GAUNTT, KBI BIOLOGY SECTION

- a soda can
- swabs of suspected blood found by the broken glass
- an item both brought to the scene and left behind at the scene by the suspect such as a hat, a glove, sunglasses, or a prying or cutting tool

Do you see the difference? DNA is transferred on **items left behind** by the suspect much more readily than by short time contact on surfaces at the scene. Many of those surfaces can better be served by looking for latent prints rather than with a swab. Yes, I realize that print powder and brushes are not as fun and are messier than swabbing a surface. But they are both the wiser choice and more successful on touched surfaces.

Both Biology and Latent Print Sections look forward to developing evidence from local contributors, making an identification, and resolving a crime. I urge the officer and deputy to look thoroughly for quality biological evidence and to speak to the reporting party or victim about items left behind at the crime scene by a suspect.

A note on crimes against person cases. We realize that on some cases, short time contact swabs might be the only items that an officer could collect at a crime scene. If the case was a crime against person, such as a sexual assault, aggravated battery, or a death investigation, the laboratory will analyze the swabs, but only after all other items of evidence have failed to associate the suspect to the crime, and after the necessary elimination DNA standards have been collected.

Property crime is more than completing an incident report and a case number for the victim's insurance claim. If the officer takes a little time to take a second look at the scene and collect quality evidence, the likelihood of solving that case increases tremendously. The KBI's dedicated examiners can take it from there.

NEWS FROM THE KBI HELP DESK

JAVIER BARAJAS, KBI HELPDESK

U.S. Commercial Driver's License Data Now Available Through Nlets

Directly from the Nlets Director of Operations desk is the following announcement.

Nlets is pleased to announce that Mexican and U.S. commercial driver's license data (CDLIS) is now available through Nlets thanks to a recently completed project in partnership with the Federal Motor Carrier Safety Administration, FMCSA. Previously, law enforcement agencies were only able to access this resource out-of-band, connecting directly to the CDLIS databases through an interface called Query Central. As a result of this project, the service is now accessible over the secure Nlets network. The service can be accessed by sending a driver's license query (DQ) and/or a driver's history query (KQ) with commercial driver's data, to the destination code CL. To support this capability a required licensed state (OLS) field has been added to the DQ transaction destined to CL. It is in this field that you will enter the state of record.

Visit http://wiki.nlets.org/index.php/Section_26:_Commercial_Vehicle_Information for more information on commercial vehicle information via Nlets.

The KBI Help Desk is in the process of adjusting the KQ and DQ message keys to accommodate the OLS field for U.S. commercial licenses.

NEWS FROM THE KBI HELP DESK-CONTINUED

JAVIER BARAJAS, KBI HELPDESK

U.S. Test records:

Message Key	Destination	Licensed State	Test Record
DQ	CL	Oklahoma	OLN: Z6TESTFHNA
KQ	CL	Oklahoma	OLN: Z6TESTFHNA

Users can now send DQ, KQ and registration queries RQ to the destination code MX, which will return the appropriate commercial driver data from the Mexico database.

Mexican Test records:

Message Key	Destination	Test Record
RQ	MX	*VIN:* **3N1BC1AS0DK218625** *VMA:* **NISS** *VYR:* **2013**
DQ	MX	*OLN:* **DF113916** *OLS:* leave blank
KQ	MX	*OLN:* **DF113916** *OLS:* leave blank

KCJIS Conference Registration

The 15th Annual Kansas Criminal Justice Information System (KCJIS) Conference is being held on June 7 – June 9, 2015 at the Ramada Inn Downtown Hotel & Convention Center, 420 E. 6th St., Topeka, KS. The registration fee is $45. The KCJIS Conference room rates are $83.00, plus tax, per night. Registrants are responsible for making their own hotel reservations: (785) 234-5400. Out-of-town registrants are encouraged to use (888) 347-2319 for hotel reservations.

Please complete a separate registration form for each person that will be attending this event by clicking "add more" on the next page. Upon submitting the registration, a confirmation page will display. Please print and retain for your records. Click here to review the Conference schedule

KCJIS User Group

At the February meeting the group received information on the Kansas Parole System from the Northern Parole Director, Mark Keating. New changes to the OpenFox Desktop Suite were presented to the group at the March meeting. The April meeting was canceled due to scheduling conflicts. Our next meeting is on May 7th, 2015 starting at 1:00PM in the Auditorium at the KBI Headquarters building in Topeka.

Java 7 Update 67

Java 7 Update 67 is now available for download via the CPI Desktop Website Feel free to update

KBI

Alicia Madison
1620 SW Tyler
Topeka, KS 66612

Phone: 785-296-3302
Email: Alicia.Madison@kbi.state.ks.us

The KCJIS NEWSLETTER is published by the Kansas

Criminal Justice Coordinating Council